

# Doubt in the Legal Capacity of Smart Contract's Parties and the Possibility of Applying the Principle of Correctness in the Assumption of Non-Qualification

Mohammad Hasan Taj Langerudi<sup>1\*</sup>, Farzin Dehdar<sup>2</sup>

1. PhD Student in Private Law, Faculty of Law, Institute for Management and Planning Studies (IMPS), Tehran, Iran.

\*Corresponding Author: Email: mohammadhasantaj@gmail.com

2. Associate Professor, Faculty of Law, Institute for Management and Planning Studies (IMPS), Tehran, Iran.

Email: f.dehdar@imps.ac.ir



S.D.I.L.  
The SD Institute of Law  
Research & Study



**Publisher:**

Shahr-e Danesh  
Research And Study  
Institute of Law

**Article Type:**

Original Research

**DOI:**

10.48300/JLR.2023.377652.2242

**Received:**

20 November 2022

**Accepted:**

17 January 2023

**Published:**

5 September 2024



## ABSTRACT

As one of the relatively new topics of the technology world, the smart contract has different angles and dimensions in the field of conclusion and execution, which must be analyzed from a legal perspective. This contract is implemented on the platform of software such as Ethereum and has features that blockchain technology benefits from. The smart contract is concluded and executed without the parties' capacities being verified, and this is considered one of its most important legal challenges in the conclusion stage. In the forward research, it is tried to introduce the mentioned feature in detail, and after providing solutions to solve this legal defect and verifying the eligibility of the parties, the criticisms of it will be expressed and it will be explained that the anonymity of the parties as one of the certain features of the smart contract should be recognized. Then this matter is

### Copyright & Creative Commons:

© The Author(s). 2021 Open Access. This article is licensed under a Creative Commons Attribution Non-Commercial License 4.0, which permits use, distribution and reproduction in any medium, provided the original work is properly cited. To view a copy of this licence, visit <https://creativecommons.org/licenses/by-nc/4.0/>.



subject to jurisprudential and legal scrutiny, whether it is possible to invoke the principle of correctness despite the lack of competence of the parties in the smart contract, or whether this transaction should be considered invalid.

**Keywords:** Blockchain, Ethereum, Smart Contract, Capacity, Principle of Correctness.

Excerpted from the Ph.D. thesis entitled "Legal Challenges of Smart Contract in Blockchain", Institute for Management and Planning Studies (IMPS), Tehran, Iran.

**Funding:** The author(s) received no financial support (funding, grants, and sponsorship) for the research, authorship, and/or publication of this article.

**Author contributions:**

Mohammad Hasan Taj Langerudi: Writing - Original Draft.

Farzin Dehdar: Writing - Review & Editing.

**Competing interests:** The authors declare that they have no competing interests.

**Citation:**

Taj Langerudi, Mohammad Hasan & Farzin Dehdar. "Doubt in the Legal Capacity of Smart Contract's Parties and the Possibility of Applying the Principle of Correctness in the Assumption of Non-Qualification". *Journal of Legal Research* 23, no. 58 (September 5, 2024): 599-630.

## Extended Abstract

Technology is introducing its new aspects at a high speed, and when these aspects are connected with the contractual relationships of people, the field of law must also analyze the challenging points and determine how to adapt the new contracts to the legal principles. One of the new issues in the world of technology is the use of blockchain. The smart contract is one of the most important products introduced to the world in the evolution of blockchain technology and has been used at an increasing speed.

To examine the issue, we are forced to provide brief definitions of some technical concepts related to smart contracts. At first, we should know that, in general, there are two main approaches in the architecture of software systems: the centralized approach and the distributed approach. In centralized software systems, system components and elements are connected to a central element that has the role of coordination and control. In contrast, a distributed system is a network of interconnected components where no central element is responsible for coordinating or controlling the other components.

Blockchain is a distributed and decentralized network of computers that is used as an advanced technology and tool to record and store information in a secure and verifiable manner.

Ethereum is a decentralized platform that was introduced in 2014 by Vitalik Buterin. In addition to the value transfer issues presented in previous generations of blockchains such as Bitcoin, Ethereum enables the execution of programs on the blockchain network by smart contracts without the intervention of a central authority.

A smart contract is referred to as a contract that is implemented on the Ethereum platform and uses blockchain distributed software system technology. It is a computer program or protocol that is designed to automatically perform specific actions such as transferring virtual assets between parties without the direct intervention of a third party, when the conditions are met.

After a brief introduction to these concepts, we should know that one of the conditions for the validity of a contract in Iranian law is that the parties should have the legal capacity. In a smart contract that is concluded on the platform of blockchain, the identity of the parties to the smart contract transaction is unknown to each other. It is clear that in this case, the parties to the transaction will remain unaware of whether the other party has the legal capacity to conclude the contract or not. In order to verify the eligibility of the parties to the smart contract, some have pointed to solutions such as "allocation of digital signatures", "allocation of license to own cryptocurrencies" and verification through "digital exchanges".

These solutions are not acceptable because one of the most important features of crypto currencies is the anonymity of the exchangers of such currencies. Other reasons for rejecting these solutions are as follows: at first, buying and selling cryptocurrencies and thus making it possible to conclude a smart contract is not done only through digital exchanges and can be done in other ways (direct purchase from the miner and purchase from Bitcoin ATMs that have been set up in some countries). Secondly, if you go to an exchange, there are decentralized and anonymous exchanges where you don't need to register your identity information, and simply by having an email address and an external wallet address, you can buy and sell cryptocurrencies easily and without restrictions. Thirdly, in addition to decentralized and anonymous exchanges, there are semi-anonymous exchanges that do not ask users for identity information and only store IP and transactions. By using these exchanges, the anonymity of people will be maintained to a large extent. Fourth, the exchange company does not provide the information to anyone, and assuming that the information is fully obtained, this information is not available to third parties who intend to buy and sell through that exchange, and for them, the identity of the other party (which according to the above explanation can be is ineligible) is unknown.

According to the above reasons and also structure of the blockchain, the identity of the parties of the smart contract remains unknown to each other, and the parties do not know whether the other party has legal capacity or not. By considering this point, this basic question arises whether in such a situation, it is possible to invoke the principle of correctness to get rid of this obstacle or not? In Islamic jurisprudence, a decisive solution has not been found to determine the scope of the implementation of the principle of correctness, and the opinions of distinguished jurists are scattered. Some believe in the implementation of the principle of correctness in assuming doubt about the parties' legal capacity, and some are against this opinion. Generally, from an Iranian legal point of view, if the parties' legal capacities are unknown, the transaction should be invalidated. Lawyers believe that the principle of correctness does not apply in the assumption that there is doubt about the legal capacities of the parties; Because that principle applies in a case where the suspicion of corruption is not related to the main elements of the contract, and the doubt in the competence of the parties to the transaction (as a pillar of the contract) prevents the implementation of the principle of integrity.

From this point of view, it can be concluded that basically, the smart contract is invalid due to the legal capacity of the parties remaining unknown, and it is not possible to implement the principle of correctness in it.

# شک در اهلیت طرفین قرارداد هوشمند و امکان اعمال اصل صحت در فرض عدم احراز اهلیت

محمدحسن تاج لنگرودی<sup>۱\*</sup>، فرزین دهدار<sup>۲</sup>

۱. دانشجوی دکتری حقوق خصوصی، دانشکده حقوق، مؤسسه عالی آموزش و پژوهش مدیریت و برنامه‌ریزی، تهران، ایران.  
\*نویسنده مسئول: a.h.mohebali@gmail.com

۲. استادیار، گروه حقوق خصوصی، دانشکده حقوق، مؤسسه عالی آموزش و پژوهش مدیریت و برنامه‌ریزی، تهران، ایران.  
f.dehdar@imps.ac.ir

## چکیده:

قرارداد هوشمند به‌عنوان یکی از موضوعات نسبتاً جدید دنیای فناوری زوایا و ابعاد مختلفی در عرصه انعقاد و اجرا دارد که ضروری است از منظر حقوقی مورد واکاوی قرار گیرد. این قرارداد در بستر نرم‌افزارهایی نظیر اتریوم به اجرا درمی‌آید و دارای ویژگی‌هایی است که فناوری بلاکچین از آن بهره‌مند است. قرارداد هوشمند بدون اینکه اهلیت طرفین در آن احراز شود، منعقد شده و به اجرا درمی‌آید و این، یکی از مهم‌ترین چالش‌های حقوقی آن در مرحله انعقاد محسوب می‌شود. در تحقیق پیش رو سعی می‌شود ویژگی مذکور به‌طور تفصیلی معرفی شود و پس از ارائه راهکارهایی برای حل این نقیصه حقوقی و احراز اهلیت طرفین، نقدهای وارد بدان بیان و این امر تبیین شود که مجهول ماندن هویت طرفین به‌عنوان یکی از ویژگی‌های مسلم قرارداد هوشمند، باید به رسمیت شناخته شود. سپس این امر مورد مذاقه فقهی و حقوقی قرار می‌گیرد که آیا با وجود محرز نبودن اهلیت طرفین در قرارداد هوشمند، امکان استناد به اصل صحت وجود

## کپی‌رایت و مجوز دسترسی آزاد:



کپی‌رایت مقاله در مجله پژوهش‌های حقوقی نزد نویسنده (ها) حفظ می‌شود. کلیه مقالاتی که در مجله پژوهش‌های حقوقی منتشر می‌شوند با دسترسی آزاد هستند. مقالات تحت شرایط مجوز 4.0 Creative Commons Attribution Non-Commercial License منتشر می‌شوند که اجازه استفاده، توزیع و تولید مثل در هر رسانه‌ای را می‌دهد، به شرط آنکه به مقاله استناد شود. جهت اطلاعات بیشتر می‌توانید به صفحه سیاست‌های دسترسی آزاد نشریه مراجعه کنید.



پژوهش‌های حقوقی



نوع مقاله:

پژوهشی

DOI:

10.48300/JLR.2023.377652.2242

تاریخ دریافت:

۲۹ آبان ۱۴۰۱

تاریخ پذیرش:

۲۷ دی ۱۴۰۱

تاریخ انتشار:

۱۵ شهریور ۱۴۰۳



دارد یا اینکه باید قائل به بطلان این معامله شد.

## کلیدواژه‌ها:

بلاکچین، اتریوم، قرارداد هوشمند، اهلیت، اصل صحت.

برگرفته از رساله دکتری با عنوان «چالش‌های حقوقی قرارداد هوشمند در بستر بلاکچین»، مؤسسه عالی آموزش و پژوهش مدیریت و برنامه‌ریزی، تهران، ایران.

**حامی مالی:**  
این مقاله هیچ حامی مالی ندارد.

**مشارکت نویسندگان:**  
محمدحسن تاج لنگرودی: نوشتن - پیش‌نویس اصلی.  
فرزین دهدار: نوشتن - بررسی و ویرایش.

**تعارض منافع:**  
بنابر اظهار نویسندگان این مقاله تعارض منافع ندارد.

## استناددهی:

تاج لنگرودی، محمدحسن و فرزین دهدار. «شک در اهلیت طرفین قرارداد هوشمند و امکان اعمال اصل صحت در فرض عدم احراز اهلیت». مجله پژوهش‌های حقوقی ۲۳، ش. ۵۸ (۱۵ شهریور ۱۴۰۳): ۵۹۹-۶۳۰.

## مقدمه

دنیای فناوری با سرعت بالایی در حال معرفی وجوه جدید خود است و هنگامی که این وجوه با روابط قراردادی افراد پیوند می‌یابد، رشته حقوق نیز ناگزیر باید ضمن واکاوی نقاط چالش‌برانگیز، نحوه انطباق قراردادهای جدید با اصول حقوقی را مشخص سازد. یکی از مسائل نوین دنیای تکنولوژی، استفاده از فناوری بلاکچین و تحولی است که به تبع آن در عرصه‌های مختلف ایجاد شده است. قرارداد هوشمند به‌عنوان یکی از مهم‌ترین محصولات است که در مسیر تکامل فناوری بلاکچین به دنیا معرفی شده و با سرعت روزافزونی مورد استفاده قرار گرفته است.

قرارداد هوشمند دارای مسائل و ابعاد مختلفی است که بررسی تمام آنها در این مختصر نمی‌گنجد و در این مقاله تنها یکی از ویژگی‌های بسیار مهم آن مورد واکاوی قرار خواهد گرفت. در این راستا متذکر می‌شویم که قرارداد هوشمند در شرایطی منعقد می‌شود که عموماً اهلیت طرفین معامله در آن احراز نمی‌شود. این ویژگی در این مقاله به‌طور تفصیلی مورد بررسی قرار خواهد گرفت و پس از بررسی ابعاد آن، با غور در آرای فقها و حقوق‌دانان درصدد پاسخ به این پرسش برخواهیم آمد که آیا می‌توان با وجود عدم احراز اهلیت طرفین، به اصل صحت استناد کرد و حکم به صحت معامله کرد یا اینکه ناگزیر از صدور حکم به بطلان معامله هستیم.

### ۱- تعاریف برخی مفاهیم

برای بررسی موضوع ناگزیر به ارائه تعاریف اجمالی از برخی مفاهیم فنی مرتبط با قرارداد هوشمند هستیم. در ابتدا باید بدانیم که به‌طور کلی، دو رویکرد اصلی در معماری سیستم‌های نرم‌افزاری وجود دارد: رویکرد متمرکز و رویکرد توزیع‌شده. در سیستم‌های نرم‌افزاری متمرکز، اجزا و عناصر سیستم به یک عنصر مرکزی که نقش هماهنگی و کنترل دارد، متصل می‌شوند. در مقابل، یک سیستم توزیع‌شده، شبکه‌ای از اجزای متصل به یکدیگر است که هیچ عنصر مرکزی، مسئولیت هماهنگی یا کنترل سایر اجزا را بر عهده ندارد.<sup>۱</sup>

#### ۱-۱- سیستم همتابه‌همتا توزیع‌شده

سیستم همتابه‌همتا<sup>۲</sup> ذاتاً یک سیستم توزیع‌شده محسوب می‌شود و شامل رایانه‌هایی است که منابع

1. Mateja Durovic & Andre Janssen, "The Formation of Smart Contracts and Beyond: Shaking the Fundamentals of Contract Law", In book Smart Contracts and Blockchain Technology: Role of Contract Law" (Cambridge: Cambridge University Press, 2019), 6.

2. Peer to Peer (P2P)

Taj Langerudi, Mohammad Hasan. "Doubt in the Legal Capacity of Smart Contract's Parties and the Possibility of Applying the Principle ...". Jour. of Legal Res. 23, no. 58 (September 5, 2024): 599-630.

محاسباتی خود را (به‌عنوان مثال قدرت پردازش، ظرفیت ذخیره‌سازی، داده‌ها یا پهنای باند شبکه) به‌طور مستقیم و بدون هیچ‌گونه مرکز هماهنگی، برای استفاده همه اعضای شبکه در دسترس قرار می‌دهند. در واقع، سرویس همتابه‌همتا، بستری غیرمتمرکز است که به‌موجب آن اعضا مستقیماً بدون واسطه و شخص ثالث با یکدیگر معامله می‌کنند. رایانه‌های سیستم همتابه‌همتا دارای مدیریت مرکزی نیستند؛ زیرا هرکدام یک کپی از فایل‌ها را در اختیار دارد و هم به‌عنوان گیرنده خدمات<sup>۳</sup> و هم به‌عنوان سرور برای سایر رایانه‌ها عمل می‌کند؛ بنابراین هر رایانه می‌تواند فایل‌ها را از سایرین دانلود یا برای آنها آپلود کند.<sup>۴</sup>

### ۱-۲- دفتر کل توزیع شده<sup>۵</sup>

دفتر کل توزیع شده، ضمن استفاده از سیستم‌های همتابه‌همتای توزیع شده، به‌عنوان شیوه‌ای برای ثبت و انتشار داده‌ها در بستر اینترنت مورد استفاده قرار می‌گیرد. سیستم دفتر کل توزیع شده دربرگیرنده پایگاه داده دیجیتالی است که بین شبکه‌ای از کامپیوترها به اشتراک گذاشته می‌شود. با توجه به اینکه ساختار دفتر کل توزیع شده مبتنی بر سیستم‌های همتابه‌همتا است، وجه تمایز آن نیز در قیاس با سایر پایگاه‌های داده در این است که فناوری مذکور توسط یک اداره‌کننده مرکزی حفظ و کنترل نمی‌شود. هیچ‌گرهی به‌طور مستقل و واحد، توان افزودن اطلاعات به دفتر کل را ندارد. یک گره می‌تواند ورود داده جدید را پیشنهاد دهد، اما داده مذکور تنها زمانی به دفتر کل اضافه می‌شود که سایر گره‌ها به این اجماع برسند که ورودی باید ثبت شود.<sup>۶</sup> هش گراف<sup>۷</sup>، هولوچین<sup>۸</sup> و بلاکچین<sup>۹</sup> از جمله انواع مختلف دفاتر کل توزیع شده محسوب می‌شوند. با توجه به اجرای قرارداد هوشمند در بستر بلاکچین در ادامه به توضیح آن خواهیم پرداخت.

### ۱-۳- بلاکچین

بلاکچین شبکه‌ای توزیع شده و غیرمتمرکز از رایانه‌ها است که به‌عنوان فناوری و ابزاری پیشرفته برای ضبط و ذخیره اطلاعات به‌صورت امن و دارای قابلیت تأیید اعتبار استفاده می‌شود. به عبارتی

3. Client

4. Gavin Zheng, *Etherium Smart Contract Development in Solidity* (Singapore: Springer, 2021), 8.

5. DLT (Distributed Ledger Technology)

6. Law Commission, *Smart legal contracts: Advice to Government* (London: Crown, 2021), 27.

7. Hashgraph

8. Holochain

9. Blockchain

بلاکچین یک دفتر کل توزیع‌شده یا پایگاه داده‌ای توزیع‌شده است که شبکه‌ای غیرمتمرکز از کامپیوترها، تراکنش‌ها را در آن ضبط می‌کنند.<sup>۱۰</sup> این فناوری توسط یک اداره‌کننده مرکزی حفظ و کنترل نمی‌شود و هیچ گرهی<sup>۱۱</sup> به‌طور مستقل و واحد، توان افزودن اطلاعات به سیستم را ندارد. یک گره می‌تواند ورود داده جدید را پیشنهاد دهد، اما داده مذکور تنها زمانی به دفتر کل اضافه می‌شود که سایر گره‌ها به این اجماع برسند که ورودی باید ثبت شود. مشکل اصلی که توسط بلاکچین حل می‌شود، دستیابی و حفظ یکپارچگی در سیستم همتابه‌همتای کاملاً توزیع‌شده است که دربرگیرنده تعداد ناشناخته‌ای از همتایان با قابلیت اتکا و اعتبار ناشناخته است.<sup>۱۲</sup> حسب توضیحاتی که در ادامه خواهد آمد، روشن خواهد شد که بلاکچین به‌عنوان یک نوآوری یکپارچه از شبکه‌های همتابه‌همتا، ضمن استفاده از امضای دیجیتال،<sup>۱۳</sup> رمزنگاری نامتقارن،<sup>۱۴</sup> هش‌نگاری<sup>۱۵</sup> و مکانیسم اجماع،<sup>۱۶</sup> مجرای قابل اعتمادی برای انتقال اطلاعات و ارزش در شبکه‌های غیرقابل اعتماد فراهم می‌کند.

### ۱-۳-۱- امضای دیجیتال در فناوری بلاکچین

امضای دیجیتال نوع پیشرفته امضای الکترونیکی است که از آن به‌عنوان امضای الکترونیکی رمزگذاری‌شده یاد می‌شود. در واقع امضای دیجیتال، امضایی است که از طریق تغییر شکل مدارک به‌صورت الکترونیکی از طریق استفاده از یک سیستم «رمزنگاری نامتقارن» و یک تابع «هش» تولید می‌شود. بلاکچین برای رفع این معضل که هم‌زمان هم باز بودن سیستم خود را حفظ کند و هم انتقال مالکیت را صرفاً محدود به صاحب حساب قانونی کند، از امضای دیجیتال بهره می‌برد.

### ۱-۳-۲- رمزنگاری نامتقارن

بلاکچین یک سیستم همتابه‌همتا است که دسترسی به آن برای همه آزاد است. هرکسی می‌تواند با ابزارهای کامپیوتری خود به آن متصل شود یا در سیستم داده، تراکنش جدیدی را ثبت کند. با این حال طبیعی است که کسی تمایل نداشته باشد افراد غریبه به اموال اختصاص‌یافته به حساب‌های

10. Aaron Wright and Primavera De Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia", SSRN, (2015), 13.

11. Node

۱۲. جواد عباسی، بلاکچین: آشنایی با مفاهیم بنیادین (تهران: مؤسسه کتاب مهربان نشر، ۱۳۹۷)، ۵۴.

13. Digital Signature

14. Asymmetric Encryption

15. Hashing

16. Consensus Mechanism

اختصاصی‌اش در بلاکچین، دسترسی داشته باشند. برای رفع این نیاز، رمزنگاری نامتقارن به کمک بلاکچین می‌آید.

در رمزنگاری نامتقارن، (برخلاف رمزنگاری متقارن که در آن برای رمزگذاری و رمزگشایی از یک کلید مشترک استفاده می‌شود) از دو کلید متفاوت استفاده می‌شود و به همین دلیل، رمزنگاری نامتقارن نامیده می‌شود.<sup>۱۷</sup> یکی از این دو کلید، «کلید عمومی»<sup>۱۸</sup> نام دارد که به‌طور گسترده در جهان منتشر می‌شود و بدون اینکه امنیت و محرمانگی پیام را به خطر اندازد در اختیار همگان قرار دارد. کلید دوم، «کلید خصوصی»<sup>۱۹</sup> نامیده می‌شود که باید نزد صاحب آن محرمانه و سری بماند.<sup>۲۰</sup> این دو کلید به لحاظ فنی مکمل و در عین حال متناظر با یکدیگر هستند؛ بدین معنا که اگر پیامی با کلید عمومی رمزنگاری شود، رمزگشایی آن تنها با کلید خصوصی مرتبط با آن امکان‌پذیر است و بالعکس، در صورت رمزنگاری پیام با کلید خصوصی، تنها با کلید عمومی متناظر آن ممکن است؛ بنابراین دو کلید در عین حال که با هم متفاوت هستند، تکمیل‌کننده یکدیگرند. کلید عمومی را می‌توان در اختیار دیگران قرار داد؛ چراکه امکان دستیابی به کلید خصوصی از طریق کلید عمومی غیرممکن است.

### ۱-۳-۳- هش‌نگاری

توابع هش<sup>۲۱</sup> یکی از مهم‌ترین فناوری‌های پایه بلاکچین است. توابع هش، برنامه‌ای کامپیوتری است که هر نوع داده‌ای را صرف‌نظر از اندازه داده ورودی، به تعداد مشخصی کاراکتر با طولی ثابت تبدیل می‌کند. توابع هش مختلفی وجود دارند که با توجه به طول مقادیر هشی که تولید می‌کنند، متفاوت هستند. یکی از گروه‌های مهم توابع هش، توابع هش رمزنگاری‌شده است که نوعی اثرانگشت دیجیتال برای هر داده تولید می‌کنند.

### ۱-۳-۴- مکانیسم اجماع

یکی از مهم‌ترین ویژگی‌های بلاکچین، غیرمتمرکز بودن آن است. بدین ترتیب، اگر اطلاعات موجود بر روی یکی از گره‌ها (همان سرورها و پردازشگرهای ثبت‌کننده و تأییدکننده اطلاعات)، به دلایل مختلف

۱۷. رسول مظاهری کوهانستانی، مطالعه تطبیقی امضای الکترونیکی در حقوق ایران و مقررات آسیترال (تهران: انتشارات جنگل، ۱۳۹۲)، ۵۷.

18. Public Key

19. Private Key

20. K. Jane Winn and Benjamin Writht, The law of Electronic Commerce (New York: Wolters Kluwer, 2002), 17.

21. Hash

از بین برود، بی‌شمار گره دیگر وجود دارد که این اطلاعات را بر روی خود ذخیره کرده‌اند. نکته حائز اهمیت این است که افزودن اطلاعات به شبکه بلاکچین باید روی تمامی گره‌ها یا سرورها اعمال شود و گره‌ها باید در خصوص افزوده شدن بلاکی جدید به شبکه به توافق برسند. اگرچه ممکن است دستیابی به توافق میان دو گره به‌سادگی امکان‌پذیر باشد، اما با وجود گره‌های متعدد که باید روی اطلاعات تراکنش واحد به اجماع برسند، این مسئله بسیار دشوار خواهد بود. برای نیل به این هدف، از مکانیسم یا الگوریتمی به نام «مکانیسم اجماع» استفاده می‌شود. در واقع، مکانیسم اجماع یا توافق عمومی همان فرایند توافق بر وضعیت نهایی داده (اطلاعات تراکنش‌ها)، توسط گره‌های سیستم توزیع شده است. به فرایند مشارکت در شبکه، همکاری در ثبت و تأیید اطلاعات و افزوده شدن بلاک‌ها به بلاکچین، فرایند «استخراج»<sup>۲۲</sup> و به فردی که این کار را انجام می‌دهد، «استخراج‌کننده»<sup>۲۳</sup> گفته می‌شود.<sup>۲۴</sup>

لازم به ذکر است که مشکل اصلی که توسط بلاکچین حل می‌شود، دستیابی و حفظ یکپارچگی در سیستم همتابه‌همتای کاملاً توزیع شده است که دربرگیرنده تعداد ناشناخته‌ای از همتایان با قابلیت اتکا و اعتبار ناشناخته است که طی آن از طریق مکانیسم اجماع، توافق عمومی حاصل می‌شود.<sup>۲۵</sup>

#### ۱-۴- اتریوم

اتریوم،<sup>۲۶</sup> بستری غیرمتمرکز است که در سال ۲۰۱۴ توسط ویتالیک بوتورین<sup>۲۷</sup> معرفی شد. علاوه بر مباحث انتقال ارزش که در نسل‌های قبلی بلاکچین مانند بیت‌کوین ارائه شده بود، اتریوم امکان اجرای برنامه‌هایی روی شبکه بلاکچین را توسط قراردادهای هوشمند<sup>۲۸</sup> بدون دخالت یک نهاد مرکزی فراهم می‌سازد. از این رو به شبکه اتریوم، بلاکچین نسل دو گفته می‌شود.<sup>۲۹</sup>

در سفیدنامه<sup>۳۰</sup> اتریوم آمده است: «جالب‌ترین نکته در مورد اتریوم آن است که پروتکل اتریوم بسیار فراتر از یک ارز است. پروتکل مربوط به ذخیره‌سازی غیرمتمرکز فایل، محاسبات غیرمتمرکز و پیش‌بینی

22. Mining

23. Miner

24. Sinclair Davidson, Primavera de Filippi & Jason Potts, Economics of Blockchain (Public Choice Conference, May 2016, Fort Lauderdale, United States)

۲۵. عباسی، پیشین، ۵۴-۷۷.

26. Ethereum

27. Vitalik Buterin

28. Smart Contracts

29. Gavin Wood, "Ethereum: A secure decentralized generalized transaction ledger", Ethereum Project Yellow Paper, 151(2014), 24.

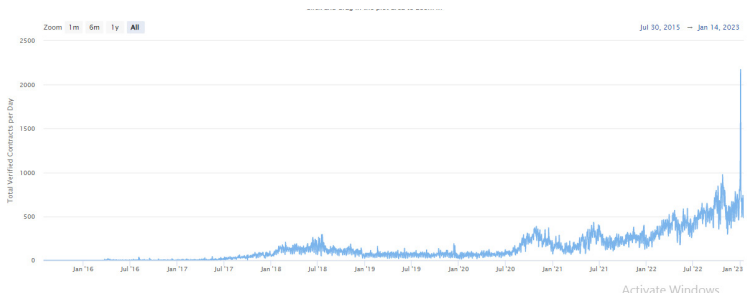
30. Whitepaper

بازارها به صورت غیرمتمرکز و بسیاری از مفاهیم این چینی، این قابلیت را دارند تا بازده صنعت رایانش را بهبود بخشند و برای اولین بار با افزودن لایه‌ای اقتصادی، موجب گسترش زیاد پروتکل‌های هم‌تا به هم‌تا شود.»

اتریوم با نداشتن پسوند کوین در نام خود به دنبال حرکتی فراتر از ایده ارز بود و در واقع در جهت رمزنگاری شدن کالا گام برداشت. در حالی که از بیت کوین اغلب برای انتقال پول میان افراد استفاده می‌شد، اتریوم برای انتقال اطلاعات میان برنامه‌ها مورد استفاده قرار گرفت. اتر نیز عنصری ضروری و همانند سوخت برای اجرای پلتفرم برنامه توزیع‌شده اتریوم است. اتر<sup>۳۱</sup> نوعی پرداخت توسط کاربران پلتفرم به ماشین‌هایی است که عملیات مورد تقاضا را انجام می‌دهند. به زبان دیگر، اتر مشوقی است که نوشتن برنامه‌های باکیفیت توسط برنامه‌نویسان و سلامت شبکه را تضمین می‌کند.

### ۱-۵- قرارداد هوشمند

اکنون با لحاظ مطالب پیش‌گفته، می‌توان به تصویر صحیح‌تری از قرارداد هوشمند دست یافت. به قراردادی که در بستر اتریوم به اجرا درمی‌آید و در این راستا از فناوری سیستم نرم‌افزاری توزیع‌شده بلاکچین، امضای دیجیتال و هش‌نگاری بهره‌مند می‌شود، قرارداد هوشمند اطلاق می‌شود. در تصویر زیر شمار قراردادهای هوشمند اجراشده در بستر اتریوم به نمایش درآمده است.<sup>۳۲</sup>



این تصویر گویای آن است که از سال ۲۰۱۵ (زمان راه‌اندازی شبکه اتریوم) تاکنون، شمار قراردادهای هوشمند اجراشده در بستر اتریوم افزایش یافته و سیر صعودی داشته است؛ به نحوی که در تاریخ ۲۸

31. Ether

32. Ethereum Daily Verified Contracts Chart, last modified Jan 14, 2023, available at <https://etherscan.io/chart/verified-contracts>.

مارس ۲۰۱۶ (۱۳۹۵/۱/۹)، صرفاً یک مورد قرارداد هوشمند در بستر اتریوم تأیید شد و به اجرا درآمد. در تاریخ دوم ژانویه ۲۰۲۳ (۱۴۰۱/۱۰/۱۲) این عدد به ۲۱۷۲ مورد رسیده است.

باید توجه داشت که تمام توضیحات و ویژگی‌هایی که برای دفتر کل توزیع‌شده، برشمرده‌ایم، شامل قرارداد هوشمند نیز می‌شود. از جمله ویژگی‌های برجسته دفتر کل توزیع‌شده این بود که فناوری مذکور توسط یک اداره‌کننده مرکزی حفظ و کنترل نمی‌شود. هیچ شخصی به‌طور مستقل و واحد، توان افزودن اطلاعات به دفتر کل را ندارد. علاوه بر این، طرفین بدون اینکه همدیگر را بشناسند یا به یکدیگر اعتماد کنند، قرارداد را منعقد می‌سازند؛ چراکه این قرارداد به‌طور خودکار و بدون نیاز به عامل انسانی اجرا می‌شود. مهم‌ترین مزیت اجرای خودکار تعهد قراردادی به‌وسیله برنامه کامپیوتری این است که با حذف دخالت عامل انسانی، دیگر شخص نمی‌تواند مانع اجرای قرارداد شود. در واقع برخلاف انسان، برنامه کامپیوتری که به‌درستی کدگذاری شده باشد، قادر به امتناع از اجرای یک تعهد نیست. هنگامی که شرایط مدنظر تحقق یابد، برنامه کامپیوتری، تعهدات قراردادی را به‌طور خودکار اجرا خواهد کرد.<sup>۳۳</sup>

قرارداد هوشمند به‌طور خودکار، تحقق شروط مندرج در قرارداد را بررسی می‌کند و پس از احراز این امر به اجرا درمی‌آید. احراز تحقق شروط از طریق اوراکل‌ها<sup>۳۴</sup> صورت می‌پذیرد. اوراکل‌ها مکانیسمی به‌منظور فراهم کردن اطلاعات مهم و قابل اعتماد برای قراردادهای هوشمند هستند. آنها به‌عنوان یک ابزار ارتباطی ایفای نقش می‌کنند که رویدادهای جهان واقعی را به داده‌های دیجیتال تبدیل می‌کنند. در واقع اوراکل‌ها، سامانه‌هایی (سرویس داده) جهت ایجاد تعامل اطلاعاتی بلاکچین و دنیای خارج از آن (صفحه گسترده جهانی) هستند. این سیستم‌ها، با استخراج اطلاعات از صفحه گسترده جهانی، آنها را به بلاکچین منتقل و در اختیار استعلام‌گیرنده قرار می‌دهند.<sup>۳۵</sup>

ضمناً به دلیل انعقاد قرارداد هوشمند در بستر یک دفتر کل توزیع‌شده، صرفاً از رمازرها به‌عنوان ثمن معامله می‌توان استفاده کرد و امکان استفاده از اسکناس یا پول‌های اعتباری و الکترونیکی منتفی است. در ادامه به ارائه برخی از مهم‌ترین تعاریف ارائه‌شده از قرارداد هوشمند می‌پردازیم.

قرارداد هوشمند، قراردادی الکترونیکی است که مطابق با ایجاب و قبول طرفین در بستر بلاکچین (زنجیره بلوکی) منعقد می‌شود.<sup>۳۶</sup>

33. Paul S. Daveis, "Smart contracts" in Contents of Commercial Contracts: Terms Affecting Freedoms (Oxford: Hart Publishing, 2020), 203.

34. Oracles

35. Thibault Schrepel, "Collusion by Blockchain and Smart Contracts", *Harvard Journal of Law and Technology*, 33, 1(2019), 39.

36. Rainer Bohme, Nicolas Christin, Benjamin Edelman and Tyler Moore, "Bitcoin: Economics,

سیستمی که به وسیله کدهای الکترونیکی، تعهدات قرار داده شده توسط طرفین قرارداد را به صورت خودکار به اجرا می‌گذارد.<sup>۳۷</sup>

برنامه دیجیتالی مبتنی بر ساختار بلاکچین که به صورت خودکار تمامی شروط و مفاد قرارداد را که تحت اراده طرفین قرار گرفته، به اجرا گذاشته و از هرگونه تغییر غیرمجاز در مفاد قرارداد توسط هریک از طرفین جلوگیری می‌کند.<sup>۳۸</sup>

[ایالت آیووا در بند ۱۴ قانون ایالتی خود در تعریف قرارداد هوشمند مقرر داشته]: قرارداد هوشمند یک پروتکل معاملاتی کامپیوتری است که بر روی یک دفتر کل توزیع شده و غیرمتمرکز اجرا می‌شود.<sup>۳۹</sup> [در قانون ایالتی آریزونا، قرارداد هوشمند این‌گونه تعریف شده است]: «برنامه‌ای که بر روی یک دفتر کل توزیع شده و غیرمتمرکز اجرا می‌شود و می‌تواند در بستر همان دفتر کل توزیع شده به انتقال دارایی بپردازد.»<sup>۴۰</sup>

[ایالت تنسی توسعه بیشتری در تعریف قرارداد هوشمند داده و در این خصوص مقرر داشته]: «برنامه کامپیوتری که بر یک دفتر کل الکترونیک توزیع شده و غیرمتمرکز به منظور اجرای خودکار، به اجرا درمی‌آید. این قرارداد شامل مواردی نظیر انتقال دارایی‌ها در این دفتر کل، ایجاد و توزیع دارایی‌های الکترونیک، ترکیب<sup>۴۱</sup> اطلاعات می‌شود (لیکن صرفاً منحصر در این موارد نیست).<sup>۴۲</sup> [گروه ویژه اقدام مالی<sup>۴۳</sup> در گزارش سال ۲۰۲۱ خود در تعریف قرارداد هوشمند بیان کرده<sup>۴۴</sup>]: یک برنامه یا پروتکل کامپیوتری است که به منظور اجرای خودکار اقداماتی مشخص نظیر انتقال دارایی‌هایی

technology, and governance”, *Journal of Economic Perspectives*, 29, 2(2015), 25.

37. Silverberg Kristen, *Getting Smart: Contracts on the Blockchain* (Washington: Institute of International Finance, 2016), 11.

38. Kristian Lauslahti, Juri Mattila & Timo Seppala, “Smart Contracts - How will Blockchain Technology Affect Contractual Practices”, *ETLA Reports*, 68(2018), 7.

39. “Smart Contract” means an event-driven program or computerized transaction protocol that runs on a distributed, decentralized, shared, and replicated ledger that executes the terms of a contract. For purposes of this subsection, “executes the terms of a contract” may include taking custody over and instructing the transfer of assets.

40. An event-driven program, with state, that runs on a distributed, decentralized, shared and replicated ledger and that can take custody over and instruct transfer of assets on that ledger.

41. Synchronize

42. An event-driven computer program, that executes on an electronic, distributed, decentralized, shared, and replicated ledger that is used to automate transactions, including, but not limited to, transactions that: (A) Take custody over and instruct transfer of assets on that ledger; (B) Create and distribute electronic assets; (C) Synchronize information.

43. Financial Action Task Group (FATF)

44. FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (Paris: Financial Action Task Group, 2021), 21.

مجازی بین طرفین بدون دخالت مستقیم شخص ثالث، در زمان تحقق شروط مدنظر، طراحی شده است.<sup>۴۵</sup>

## ۲- احراز اهلیت طرفین در قرارداد هوشمند

یکی از شرایط اعتبار عقد این است که طرفین، صلاحیت انجام عمل حقوقی و در واقع، قابلیت داشتن حق و توان تصرف در آن را دارا باشند. این وصف را در اصطلاح «اهلیت» می‌نامند که با شخصیت و تکامل قوای دماغی و شعور اشخاص ارتباط کامل دارد و شرط وجود و سلامت اراده نیز هست.<sup>۴۶</sup>

اهلیت دارای دو وجه است: نخست اهلیت تمتع (دارا شدن حق) که در واقع استعدادی است که به موجب آن شخص از حقوق خصوصی بهره‌مند می‌شود و می‌تواند صاحب حق و تکلیف شود. این اصطلاح بارها در قانون مدنی بکار رفته است. (مواد ۹۵۷، ۹۵۸، ۹۵۹ و ۹۶۱) برخی اساتید حقوق نیز از آن با عنوان اهلیت تملک یاد کرده‌اند.<sup>۴۷</sup> دوم، اهلیت استیفا (تصرف، اجرای حق) که صلاحیتی است که شخص به حکم قانون درباره اعمال حق خویش می‌باید. حقوق دانان بر این باورند که از آنجا که قواعد مربوط به اهلیت با مصلحت جامعه ارتباط دارند و دارای اهمیت خاصی هستند، از قواعد آمره و مربوط به نظم عمومی محسوب می‌شوند و افراد نمی‌توانند بر خلاف آن توافق کنند.<sup>۴۸</sup>

فضای مجازی فی‌نفسه زمینه پنهان ماندن هویت افراد را فراهم می‌سازد و افراد می‌توانند به دلایل مختلف، با پنهان نگاه داشتن هویت واقعی خود و ارائه یک هویت کاذب، وارد تعاملات گوناگون با یکدیگر شوند. یکی از امور تسهیلگر در راستای شناسایی افراد در فضای مجازی، نهادهای واسطی هستند که به دلایل مختلف و به طرق گوناگون اقدام به شناسایی هویت افراد می‌کنند و همگان با اتکا به این نهادها، به تعامل با یکدیگر می‌پردازند؛ این در حالی است که ساختار بلاکچین، حسب توضیحات پیشین، بر اساس غیرمتمرکز بودن و حذف نهادهای واسطی قوام یافته است. بلاکچین با توزیع داده‌ها میان همه کاربران و ارائه شفافیت گسترده، سعی کرده ضمن تمرکززدایی از یک نهاد واسطی، بدون

45. A smart contract is a computer program or a protocol that is designed to automatically execute specific actions such as VA transfer between participants without the direct involvement of a third party when certain conditions are met.

۴۶. ناصر کاتوزیان، دوره حقوق مدنی، قواعد عمومی قراردادها (انعقاد و اعتبار قرارداد نظریه بطلان و عدم نفوذ) (تهران: شرکت سهامی انتشار، ۱۳۹۴)، ۷.

۴۷. همان، ۸.

۴۸. سیدحسین صفایی، حقوق مدنی: قواعد عمومی قراردادها (تهران: میزان، ۱۳۹۷)، ۱۵.

شناسایی هویت افراد، زمینه تعاملات صحیح را فراهم سازد. با این توضیح و لحاظ این ویژگی ذاتی بلاکچین باید بیان کنیم که در قرارداد هوشمند که در بستر بلاکچین منعقد می‌شود، اولاً و بالذات، هویت طرفین معامله برای یکدیگر، تفصیلاً و اجمالاً مخفی باقی خواهد ماند. روشن است که در این صورت طرفین معامله نسبت به این امر که طرف مقابل از اهلیت لازم برای انعقاد قرارداد برخوردار است یا خیر، ناآگاه باقی خواهند ماند. در صورتی که بخواهیم از این نقیصه رهایی بجوییم باید متوسل به ابزارهای ثانویه بشویم و در خصوص امکان بهره‌مندی از آنها در این راستا مذاقه کنیم. در این خصوص و به‌ویژه برای احراز اهلیت طرفین معامله، برخی نویسندگان حقوقی به راهکارهایی اشاره کرده‌اند. در ادامه ضمن اشاره اجمالی به راهکارهای موجود، صحت و سقم توسل به آنها به منظور حل این مسئله را بررسی می‌کنیم.

## ۲-۱- شیوه‌های احراز اهلیت

برخی برای احراز اهلیت طرفین قرارداد هوشمند به راهکارهایی نظیر «تخصیص امضانات دیجیتالی»، «تخصیص مجوز تملک ارزهای رمزنگاری‌شده» و احراز از طریق «صرافی‌های دیجیتالی» اشاره کرده‌اند که به بررسی آنها خواهیم پرداخت.

### ۲-۱-۱- احراز از طریق تخصیص امضانات دیجیتالی

«از جمله شرایط اساسی برای انعقاد قراردادهای هوشمند، به‌کارگیری امضای دیجیتال است. در واقع در این قراردادها تا زمانی که مفاد قرارداد به‌وسیله کلید خصوصی اختصاص‌یافته به افراد امضا نشود، قراردادی تشکیل نمی‌گردد. در کشورهای توسعه‌یافته اختصاص مجوز استفاده از این نوع امضا، منوط به شناسایی هویت فرد متقاضی است.»<sup>۴۹</sup> برخی از نویسندگان غیرحقوقی نیز به تبعیت از نوشته فوق، ضمن طرح این پرسش که «آیا در قراردادهای هوشمند، سیستم شناسایی و احراز اهلیت قانونی لازم برای طرفین انعقاد قرارداد وجود دارد؟» این‌گونه پاسخ داده‌اند: «در پیش از انعقاد قرارداد، داشتن مجوز امضای دیجیتال و امکان استفاده و انتقال رمزارز به افراد این نقش را ایفا می‌کند. در این وضعیت، اعطای این مجوزها منوط به احراز هویت و اهلیت متقاضیان است و در غیر این صورت، مجوزی صادر نمی‌شود. در این حالت، اگر فردی محجور بوده یا اهلیت وی در انعقاد این قراردادها مخدوش باشد،

۴۹. همایون مافی و مهدی ناصر، «واکاوی مکانیسم احراز اهلیت متعاملین در پیاده‌سازی قراردادهای هوشمند در حقوق ایران»، پژوهشنامه بازرگانی، ۲۵، ۹۸ (۱۴۰۰)، ۲۸۹.

طبیعتاً مجوز امضای دیجیتال و امکان استفاده و انتقال رمزارز به وی تعلق نخواهد گرفت.<sup>۵۰</sup>

## ۲-۱-۲- احراز از طریق تخصیص مجوز تملک ارزهای رمزنگاری شده

«یکی دیگر از روش‌های احراز اهلیت افراد برای انعقاد قراردادهای هوشمند، پیش‌بینی تشریفات تخصیص امکان تملک ارزهای رمزنگاری شده توسط متقاضی است. با تصویب کنوانسیون یکنواخت‌سازی معاملات مبتنی بر ارزهای دیجیتال در سال ۲۰۱۷،<sup>۵۱</sup> تخصیص امکان تملک ارزهای دیجیتال به افراد متقاضی، منوط به تقدیم مدارکی نظیر سوابق محکومیت‌های کیفری و حقوقی، سوابق ورشکستگی، مایملک و ... مطابق با شرایط ماده ۲ کنوانسیون است.<sup>۵۲</sup> به عبارت دیگر در صورتی که فردی تمایل به انعقاد قراردادهای الکترونیکی مبتنی بر ارزهای دیجیتال داشته باشد، باید نسبت به اخذ شرایط بند دوم از ماده ۲ کنوانسیون اقدام کند. یکی از شرایطی که در این ماده ذکر شده، برخورداری از اهلیت معامله توسط فردی است که متقاضی تملک این نوع ارزها باشد.»<sup>۵۳</sup>

## ۲-۱-۳- احراز اهلیت از طریق صرافی‌های دیجیتال

راهکار دیگری که می‌توان برای احراز اهلیت افراد بدان تمسک جست، شیوه‌ای است که هم‌اکنون در صرافی‌های دیجیتال انجام می‌شود. صرافی‌ها، ارائه مدارک معتبر شناسایی را شرط ثبت نام افراد و بهره‌مندی از امکان خریدوفروش رمزارز، قرار داده‌اند. در این راستا، می‌توان صرافی‌ها را الزام نمود ضمن احراز هویت افراد، اهلیت اشخاص متقاضی را نیز مدنظر قرار داده و پس از احراز آن، امکان خریدوفروش رمزارزها را برای متقاضیان فراهم سازند.

## ۲-۲- نقد راهکارهای پیشنهادی در احراز اهلیت طرفین

پیش از ورود به نقد بنیادین راهکارهای پیشنهادی متذکر می‌شویم که ارائه‌دهنده محترم دو راهکار

۵۰. رسول خوانساری و وهاب قلیچ، بررسی ابعاد فقهی و حقوقی به‌کارگیری قراردادهای هوشمند در نظام مالی ایران (گزارش

سیاستی) (تهران: پژوهشکده پولی و بانکی بانک مرکزی جمهوری اسلامی ایران، ۱۳۹۹)، ۱۴.

51. Uniform Regulation Virtual Currency Business Act, July 2017 (URVCBA)

52. (URVCBA Article2): A person may not engage in virtual-currency business activity, or hold itself out as being able to engage in virtual-currency business activity, with or on behalf of a resident unless the person is: (1) licensed in this state by the department under Section 202; (2) licensed in another state to conduct virtual-currency business activity by a state with which this state has a reciprocity agreement and has qualified under Section 203; (3) registered with the department and operating in compliance with Section 207; or (4) exempt from licensure or registration under this [act] by Section 103(b) or (c).

۵۳. مافی و ناصر، پیشین، ۲۹۶.

نخست، امکان تحقق هردو مورد را در ایران به دلیل فقدان شرایط قانونی و اجرایی لازم دشوار تلقی می‌کند. در خصوص مورد اول، (احراز از طریق تخصیص امضائات دیجیتالی)، به این امر اشاره می‌کند که «با توجه به اینکه یکی از شرایط تخصیص امضای الکترونیکی مطمئن در نظام حقوقی ایران مطابق آنچه در بند ب ماده ۱۰ قانون تجارت الکترونیکی مصوب ۱۳۸۲ ذکر شده، تشخیص هویت افراد است، بالطبع تجویز استفاده از این امضا به افراد منوط به دارا بودن برخی شرایط از جمله اهلیت تمتع و استیفا است. اصولاً در صورت از بین رفتن اهلیت تمتع یا استیفا، مجوز استفاده از این امضا باید ابطال شود؛ این در حالی است که در نظام حقوقی کشورمان، ضوابط این امر تبیین نشده است. نتیجه این است که در صورتی که فردی موقتاً فاقد اهلیت استیفا یا تمتع در کشور ایران شود، اگر واجد مجوز استفاده از امضائات الکترونیکی مطمئن باشد، این مجوز باطل نخواهد شد. این امر امکان سوءاستفاده را نیز فراهم می‌سازد. در صورتی که تجار داخلی یا خارجی، به اعتبار امضائات الکترونیکی مطمئن مورد استفاده توسط یکی از بازرگانان ایرانی، مبادرت به انعقاد قراردادهای کلان با وی کرده و پس از آشکار شدن کلاهبرداری صورت گرفته، وجوه طرف قرارداد در معرض تلف قرار گیرد، نه مکانیسمی حمایتی جهت مسئولیت دولت بر نظارت بر نحوه استفاده از امضائات الکترونیکی مطمئن در کشور ایران طراحی شده است، نه می‌توان از چنین سوءاستفاده‌های جلوگیری کرد. تنها حکمی که قانون‌گذار ایران در این خصوص پیش‌بینی کرده، قواعد عام موجود در قانون مدنی بر ابطال معاملات غیرنافذ یا تقاضای اعلام بطلان قرارداد توسط دادگاه است. این ضمانت اجرا به جهت عدم کارایی سریع در جبران خسارت وارد به طرف دیگر قرارداد، نه تنها اعتبار تجار ایرانی در معاملات فرامرزی را تحت الشعاع قرار می‌دهد، بلکه مکانیسم پیاده‌سازی ابزارهای نوین مبادلاتی در کشور ایران را نیز با چالش‌های جدی مواجه می‌سازد.»<sup>۵۴</sup>

وی همچنین در نقد مورد دوم (احراز از طریق تخصیص مجوز تملک ارزهای رمزنگاری شده) بیان می‌دارد که «در ایران سیاست‌گذاری قانونی در راستای اعتبارسنجی ابزارهای دیجیتال صورت نگرفته است.» و در این راستا به خصوص به نواقص قانون پولی و بانکی مبنی بر اینکه صرفاً سکه‌های فلزی و اسکناس را پول رایج کشور تلقی کرده و ارزهای رمزنگاری شده را به رسمیت نشناخته است، اشاره می‌کند.

آنچه در خصوص مطالب این نگارنده محترم باید بدان توجه داشت این است که ایشان بدون لحاظ ویژگی‌های اصلی و ذاتی بلاکچین، در صدد احراز اهلیت طرفین معامله برآمده است. همان‌طور که بیان

شد، بلاکچین یکی از انواع دفتر کل توزیع شده است. در این فناوری، افراد با کدهای کامپیوتری با هم در تعامل هستند؛ کما اینکه در بسیاری دیگر از فناوری‌ها نیز همین گونه است، لیکن وجه تمایز بلاکچین با سایر فناوری‌ها در این است که بلاکچین سعی کرده با ارائه مدل جدیدی از شفافیت، مانع ارتکاب اعمال خلاف شود و با قابلیت‌هایی که ارائه داده، احتمال تقلب در معامله را کاهش دهد. اگرچه اقدامات تقنینی (نظیر قواعد و قوانین مختلف ولو اندک وضع شده توسط کشورهای مختلف) و اجرایی (نظیر رویکرد برخی صرافی‌ها مبنی بر لزوم ارائه کارت شناسایی هنگام ثبت نام) تا حدودی این معضل را حل کرده، اما توانایی حل کامل آن را نخواهد داشت.

همان‌طور که پیش‌تر به تفصیل اشاره شد، یکی از مهم‌ترین ویژگی‌های ارزهای رمزنگاری شده، مجهول ماندن هویت مبادله‌کنندگان این گونه ارزهاست. هرچند هر کیف پول که در زنجیره بلوکی وجود دارد، در دسترس عموم است، اما انتساب هر یک از کیف پول‌ها به فردی معین که دارنده آن است، بسیار دشوار است. در واقع باید مدعی شد که مشکل مجهول ماندن هویت افراد در قرارداد هوشمند، معضلی نیست که با اصلاح قوانین و مقررات یا زیرساخت‌های فنی قابل رفع باشد؛ حاکمیت به هر راهکاری نیز متوسل شود، امکان فعالیت افراد خارج از این چهارچوب وجود دارد؛ اگرچه مستنبط از مواد ۳۱، ۳۲ و ۶۸ قانون تجارت الکترونیک مصوب ۱۳۸۲<sup>۵۵</sup> و آیین‌نامه اجرایی ماده ۳۲ قانون مذکور<sup>۵۶</sup> مصوب ۱۳۸۲

۵۵. ماده ۳۱ - دفاتر خدمات صدور گواهی الکترونیکی واحدهایی هستند که برای ارائه خدمات صدور امضای الکترونیکی در کشور تأسیس می‌شوند. این خدمات شامل تولید، صدور، ذخیره، ارسال، تأیید، ابطال و به‌روز نگه‌داری گواهی‌های اصالت (امضای الکترونیکی می‌باشد. ماده ۳۲ - آیین‌نامه و ضوابط نظام تأسیس و شرح وظایف این دفاتر توسط سازمان مدیریت و برنامه‌ریزی کشور و وزارتخانه‌های بازرگانی، ارتباطات و فناوری اطلاعات، امور اقتصادی و دارایی و دادگستری تهیه و به تصویب هیئت‌وزیران خواهد رسید. ماده ۶۸ - هرکس در بستر مبادلات الکترونیکی، از طریق ورود، تغییر، محو و توقف «داده‌پیام» و مداخله در پردازش «داده‌پیام» و سیستم‌های رایانه‌ای و یا استفاده از وسایل کاربردی سیستم‌های رمزنگاری تولید امضا - مثل کلید اختصاصی - بدون مجوز امضاکننده و یا تولید امضای فاقد سابقه ثبت در فهرست دفاتر اسناد الکترونیکی و یا عدم انطباق آن وسایل با نام دارنده در فهرست مزبور و اخذ گواهی مجعول و نظایر آن اقدام به جعل «داده‌پیام»‌های دارای ارزش مالی و اثباتی نماید تا با ارائه آن به مراجع اداری، قضایی، مالی و غیره به‌عنوان «داده‌پیام»‌های معتبر استفاده نماید جاعل محسوب و به مجازات حبس از یک تا سه سال و پرداخت جزای نقدی به میزان پنجاه میلیون ریال محکوم می‌شود.

۵۶. ماده ۱۱ - کلیه مؤسسات اعم از دولتی یا غیردولتی می‌توانند در حوزه فعالیت داخلی خود بدون اخذ مجوز از مرکز ریشه مبادرت به ثبت و صدور گواهی نمایند. گواهی‌هایی که به این صورت صادر می‌شود خارج از شمول مقررات این آیین‌نامه بوده و امضاهایی که به‌وسیله این گواهی‌ها تأیید می‌شوند خارج از موضوع ماده (۱۰) قانون و صرفاً قابل استفاده در همان مؤسسات خواهد بود.

این است که افراد برای امضای دیجیتال ملزم به مراجعه به مراکز صدور گواهی الکترونیکی هستند، لیکن نکته حائز اهمیت این است که در عمل و مقام اجرا، افراد بدون مراجعه به این مراکز نیز توان صدور امضای دیجیتال را برای خود دارند. شاید این ایراد مطرح شود که در این صورت حاکمیت اثری را بر این امضا مترتب نخواهد ساخت. در این خصوص باید به این امر مهم توجه داشت که با توجه به قابلیت خوداجرایی قرارداد هوشمند و پیش‌بینی امکان فسخ ابتدایی در آن طرفین قرارداد چه نیازی برای مراجعه به حاکمیت و شناسایی قراردادشان دارند؟ طرفین قرارداد در صورتی خود را نیازمند به مراجعه به محاکم می‌دانند که طرف مقابل از اجرای تعهدات خود سرباز زند؛ هنگامی که چنین فرضی در این قرارداد منتفی است، به تبع نوع رویکرد حاکمیت نسبت به این قرارداد نیز وجهی نخواهد داشت.

افزون بر موارد فوق، به راهکار مطرح‌شده مبنی بر احراز هویت افراد از طریق صرافی‌های دیجیتال نیز نقدهای جدی زیر وارد است.

نخست اینکه خریدوفروش رمزارز و به تبع مهیا شدن امکان انعقاد قرارداد هوشمند صرفاً از طریق صرافی‌های دیجیتال انجام نمی‌شود و می‌توان از طرق دیگر (خرید مستقیم از شخص ماینر و خرید از خودپردازهای بیت‌کوین که در برخی کشورها راه‌اندازی شده) نیز اقدام کرد.

دوم اینکه در صورت مراجعه به صرافی، صرافی‌های غیرمتمرکز و ناشناس وجود دارند که نیازی به ثبت اطلاعات هویتی در آنها نیست و صرفاً با داشتن یک آدرس ایمیل و یک آدرس والت بیرونی می‌توان به راحتی و بدون محدودیت اقدام به خریدوفروش رمزارزها کرد. از معروف‌ترین صرافی‌های ناشناس موجود باید به بیت‌مکس،<sup>۵۷</sup> بیت‌کوینک<sup>۵۸</sup> و بیسک<sup>۵۹</sup> اشاره کرد.

سوم اینکه افزون بر صرافی‌های غیرمتمرکز و ناشناس، صرافی‌های نیمه‌ناشناس وجود دارند که از کاربران اطلاعات هویتی نمی‌خواهند و صرفاً آی‌پی و تراکنش‌های صورت‌گرفته را ذخیره می‌کنند. با استفاده از این صرافی‌ها تا حد زیادی، ناشناس بودن افراد حفظ خواهد شد. معروف‌ترین صرافی نیمه‌ناشناس موجود کوین‌بیس<sup>۶۰</sup> است.

چهارم اینکه در صورت مراجعه به صرافی‌هایی که ارائه کارت شناسایی را شرط ثبت‌نام قرار داده‌اند، باز هم مشکلی حل نمی‌شود؛ چراکه این شرکت‌ها شرطی مبنی بر این قرار نداده‌اند که افرادی که لزوماً اهلیت دارند، امکان ثبت‌نام دارند. اساساً عمده دلیل درخواست اطلاعات از سوی صرافی‌ها

57. Bitmex

58. Bitquick

59. Bisq

60. Coinbase

این است که مانع اقدامات مجرمانه و پول‌شویی افراد و گروه‌های تبهکار شوند و از این منظر، شناسایی اهلیت فرد، واجد اهمیت نیست.

پنجم اینکه شرکت صرافی اطلاعات را در اختیار کسی قرار نمی‌دهد و بر فرض اخذ کامل اطلاعات، این اطلاعات در اختیار افراد ثالثی که قصد خرید و فروش از طریق آن صرافی را دارند، قرار نگرفته و همچنان برای آنها هویت طرف مقابل (که حسب توضیحات فوق می‌تواند فاقد اهلیت باشد) مجهول است.

در تأیید این برداشت که امکان احراز هویت افراد در قرارداد هوشمند با صعوبت و دشواری مواجه است، اشاره به گزارشی که گروه ویژه اقدام مالی<sup>۶۱</sup> برای وزرای اقتصاد گروه جی ۲۰<sup>۶۲</sup> تدارک دیده بود،<sup>۶۳</sup> حائز اهمیت است. در این راستا آمده است که «توسعه شفافیت و دسترسی به اطلاعات مالکیت ذی‌نفعان ارزشهای مجازی همچنان از اولویت بالایی برخوردار است. کشورهای اندکی توانسته‌اند این امکان را فراهم سازند که اطلاعات مالکان در اختیار مقامات صالحه قرار گیرد.»<sup>۶۴</sup>

در بیانیه حقوقی منتشرشده از سوی کارگروه قضایی بریتانیا<sup>۶۵</sup> (که با حمایت دولتی به‌منظور حمایت از تحول حقوق بریتانیا در حوزه فناوری فعالیت می‌کند) ضمن مفروض انگاشتن این امر که طرفین معامله در قرارداد هوشمند برای یکدیگر ناشناس هستند، تصریح شده که این امر در حقوق انگلستان محل نزاع و بررسی نیست؛ چراکه طرفین پذیرفته‌اند حسب اصول مندرج در قرارداد هوشمند با یکدیگر قراردادی را منعقد کنند.<sup>۶۶</sup>

در گزارش کمیسیون اقتصادی مجلس شورای اسلامی کشورمان درباره رمزارزها که در تاریخ ۱۴۰۰/۰۶/۲۳ در صحن علنی مجلس قرائت شد نیز بدین امر تأکید شد که ماهیت نامتمرکز رمزارزها و تأکید فعلی بر ناشناس بودن دارندگان و مبادله‌کنندگان و عدم احراز هویت آنها، بزرگ‌ترین چالش فراروی

61. Financial Action Task Group (FATF)

62. G20

63. FATF, FATF Report to G20 Finance Ministers and Central Bank Governors (Paris: Financial Action Task Group, 2018), 7.

64. Improving the transparency and availability of beneficial ownership information remains a high priority. Through the FATF mutual evaluation process to-date, few countries have demonstrated that information is available to competent authorities on the beneficial owner of legal persons and arrangements, or that these persons and arrangements are prevented from being misused.

65. UK Jurisdiction Taskforce, Legal Statement on Cryptoasset and Smart Contracts (London: The LawTech Delivery Panel, 2019), 8.

66. English law does not struggle with the concept of anonymous or pseudonymous parties contracting; nor with the notion that a contract can be formed between individuals by virtue of them each having agreed to subscribe to a set of rules (as happens, for example, in a club).

کشورها برای تصمیم‌گیری در این حوزه است.

مجدداً خاطرنشان می‌سازد که بر فرض دستیابی به اطلاعات مالکان (که با دشواری مواجه است) اساساً احراز اهلیت طرفین محلی از اعراب ندارد؛ بلکه صرفاً فهم و کشف این مهم است که فردی که اقدام به خرید و فروش ارزهای رمزنگاری شده می‌کند، تبعه کدام کشور بوده و آیا از آن در راستای اقدامات مجرمانه و پول‌شویی بهره می‌برد یا خیر.

در پایان متذکر می‌شویم که اگرچه حسب ماده ۵۸۸ قانون تجارت، اشخاص حقوقی متمتع از حقوق مدنی بوده و قابلیت اجرای حقوق و انجام تکالیف خود را، جز آنکه مختص اشخاص طبیعی باشد، دارند و از همین رو، اهلیت اشخاص حقوقی نیز مباحث گسترده‌ای را در عالم حقوق به خود اختصاص داده؛ لیکن منطقاً و نیز حسب نص ماده ۵۸۹ قانون تجارت، تصمیمات شخص حقوقی به‌وسیله مقاماتی که به موجب قانون یا اساسنامه تعیین شده باشند، اخذ می‌شود. این امر مبین اظهار اراده شخص حقوقی و اجرای حقوق و تعهدات وی توسط نمایندگان قراردادی یا قانونی این شخص است. با توجه به اینکه در قراردادهایی که از طریق نمایندگی منعقد می‌شود، اهلیت نماینده جزء ارکان عقد بوده<sup>۶۷</sup> و باید در هنگام انعقاد عقد به‌صورت کامل وجود داشته باشد، هر آنچه پیش‌تر در خصوص نحوه احراز اهلیت اشخاص حقیقی مطرح کردیم، در خصوص اشخاص حقوقی نیز صادق بوده و به همین دلیل از اختصاص بخشی مجزا به احراز اهلیت اشخاص حقوقی امتناع ورزیدیم.

### ۳- امکان اجرای اصل صحت در صورت مجهول بودن هویت طرفین برای یکدیگر

همان‌طور که در بخش پیش شرح داده شد، با توجه به ساختار و اقتضائات بلاکچین، هویت طرفین قرارداد هوشمند برای یکدیگر مجهول باقی می‌ماند و طرفین علم اجمالی نیز نسبت به این امر ندارند که آیا طرف مقابل واجد اهلیت است یا خیر. در این راستا این سؤال اساسی بروز می‌کند که آیا در چنین شرایطی، امکان استناد به اصل صحت برای رهایی از این مانع وجود دارد یا خیر؟

پیش از ورود به بحث باید متذکر شویم که منشأ تردید در صحت و فساد قرارداد، گاه به شبهه‌ای حکمی و گاه به شبهه‌ای موضوعی بازمی‌گردد. شبهه حکمی در جایی است که حکم کلی شرعی نسبت به موضوعی روشن نباشد. منشأ این شبهه یا به سبب نبودن دلیل قانونی، یا اجمال دلیل یا به سبب

۶۷. عبدالحسین شیروی و مرتضی محمدی، «تشکیل قراردادها از طریق نمایندگی سامانه هوشمند»، حقوق تطبیقی، ۱۶ (۱۳۸۸)، ۲۴.

تعارض ادله رخ می‌دهد؛<sup>۶۸</sup> برای مثال قراردادی واقع می‌شود که نهاد و سنخ آن در قوانین پیش‌بینی نشده است؛ نظیر بیمه، فروش سرقفلی و انتقال حق تألیف و اختراع و در این راستا این پرسش مطرح می‌شود که آیا حکم عام «لزوم وفای به عقد» شامل این‌گونه قراردادها نیز می‌شود یا صرفاً منحصر در عقود معین است؟ مستنبط از ماده ۱۰ قانون مدنی این است که همه قراردادها جز در موردی که خلاف صریح قانون است (یعنی تردیدی در مخالفت آن با قانون وجود ندارد) نافذ هستند. افزون بر اینکه، در این بخش از پژوهش، با شبهه‌ای موضوعی مواجهیم و پرداختن به شبهه حکمی و مشروعیت عقود غیرمعین وجهی ندارد؛ لذا آنچه در این بخش مدنظر است، بررسی اجرای اصل صحت در شبهات موضوعی است.

### ۳-۱- آرای فقها

در فقه راه‌حل قطعی برای تعیین قلمروی اجرای اصل صحت پیدا نشده و نظرات فقهای بزرگوار، متشکک است. برخی قائل به اجرای اصل صحت در فرض تردید نسبت به اهلیت طرفین بوده و برخی مخالف این نظر هستند. موافقین برآنند که تنها شرط اجرای اصل صحت، وقوع عرفی معامله است و پس از آن، تردید نسبت به اهلیت طرفین، خدشه‌ای به صحت معامله وارد نمی‌سازد. عمده استدلال فقهای مخالف نیز آن است که اصل صحت در موردی جاری می‌شود که شک در فساد، ناظر به ارکان اصلی عقد نباشد و شک در اهلیت طرفین معامله (به‌عنوان رکن عقد) مانع اجرای اصل صحت است.

### ۳-۱-۱- اجرای اصل صحت در فرض تردید نسبت به اهلیت طرفین

برخی فقیهان بر این باورند که اصل صحت در تمام مواردی که شک در صحت و فساد معامله واقع شده وجود دارد، معتبر است، خواه ادعای فساد ناظر به وجود مانع صحت یا فقدان شرط آن یا عدم اهلیت یکی از دو طرف یا عدم صلاحیت یکی از دو عوض باشد.<sup>۶۹</sup> و<sup>۷۰</sup> بنابراین تنها شرط اجرای اصل صحت وقوع عرفی معامله موردنظر است و درباره معامله واقع شده هیچ امتیازی بین شروط مربوط به عقد و شرایط اهلیت و دو عوض نیست و برخورد با هیچ اصلی، هرچند استصحاب، دامنه اجرای اصل صحت را محدود نمی‌سازد.

۶۸. علی مشکینی، المنافع العامه (تهران: انتشارات یاسر، ۱۳۴۸)، ۸۳.

۶۹. محمدحسن نجفی، جواهر الکلام فی شرح شرائع الإسلام، جلد ۲۳ (قم: مؤسسه نشر اسلامی، ۱۴۳۲ق)، ۱۹۴.

۷۰. مرتضی انصاری، فرائد الاصول (قم: مجمع الفکر الاسلامی، ۱۴۱۹)، ۹۶.

### ۳-۱-۲- عدم اجرای اصل صحت در فرض تردید نسبت به اهلیت طرفین

بسیاری از فقها قائل بر این هستند که در صورت تردید در خصوص اهلیت طرفین، مجرای برای اصل صحت وجود ندارد. فقهای قائل به این نظر، با مبانی مختلف به تبیین رأی خود پرداخته‌اند.

گروهی از فقیهان اصل صحت را در موردی جاری دانسته‌اند که شک در فساد ناظر به ارکان اصلی عقد (دو طرف معامله و دو عوض) نباشد: ریشه این نظر در مبسوط شیخ طوسی است و دیگران از او اقتباس کرده‌اند.<sup>۷۱</sup> علامه حلی در قواعد (کتاب ضمان) می‌نویسد: «ضمان کودک از دیگری صحیح نیست هرچند که ولی به او اذن داده باشد، پس اگر ضامن و مضمون له در باره بلوغ او اختلاف پیدا کردند (بدین معنی که آیا ضامن در دوران کودکی ملتزم شده است یا در حال کمال) گفته ضامن مقدم است؛ زیرا اصل برائت و اصل عدم بلوغ موافق با آن است و مدعی اهلیت (مضمون له) نه اصلی دارد که بدان استناد جوید نه ظاهری که بدان رجوع کند، به خلاف آنکه ادعا شود شرطی فاسد است؛ زیرا ظاهر این است که آن دو تصرف باطلی نمی‌کنند. همچنین است در مورد کسی که جنون او ثابت شده است.»<sup>۷۲</sup> باید دانست که علامه حلی در همان کتاب قواعد و در مسائل مورد نزاع بیع، در این فرض که بایع ادعا کند به هنگام فروش کودک بوده است، می‌نویسد: «احتمال دارد که گفته مدعی صحت با سوگند مقدم باشد یا گفته فروشنده به دلیل اصالت بقا».<sup>۷۳</sup>

برخی فقها بر این باورند که چون مبنای اصل صحت «اجماع» است، باید آن را به مواردی اختصاص داد که اهل فتوا اتفاق نظر دارند. بر این پایه، هرگاه شک در فساد ناشی از تردید در شرایط عقد باشد (مانند موالات) اصل صحت به طور مطلق جاری می‌شود، ولی در شرایط طرفین، اهلیت تابع اصل قرار نمی‌گیرد. در شرایط دو عوض نیز در آنجا که مربوط به داشتن مالیت و قابلیت انتقال است، اصل صحت جاری نمی‌شود.<sup>۷۴</sup>

### ۳-۲- آرای حقوق دانان

همچون فقه، در حقوق نیز اختلاف نظر میان آرای حقوق دانان مشهود است که در ادامه مورد بررسی قرار می‌گیرد.

۷۱. محمدبن حسن طوسی، المبسوط فی فقه الامامیه، جلد ۲ (قم: دفتر انتشارات اسلامی، ۱۳۸۶)، ۳۳۶.

۷۲. حسن بن یوسف حلی، قواعد الاحکام (قم: دفتر انتشارات اسلامی، ۱۳۷۰)، ۷۴۲.

۷۳. سیدمحمدجواد حسینی عاملی، مفتاح الکرامه فی شرح قواعد العلامه (قم: دفتر انتشارات اسلامی، ۱۳۹۱)، ۷۶۵.

۷۴. محمدحسین نائینی، فوائد الاصول، جلد ۴ (دفتر انتشارات اسلامی، ۱۳۷۶)، ۲۴۵.

### ۳-۲-۱- اجرای اصل صحت در فرض تردید نسبت به اهلیت طرفین

برخی حقوق‌دانان، ضمن عام تلقی کردن اصل صحت، گستره شمول آن را توسعه می‌دهند. دکتر کاتوزیان در این خصوص آورده: «با مبنایی که ما برای اصل صحت برگزیدیم، بایستی آن را عام دانست و به دنبال استثنای احتمالی رفت. منتها، این شرط عقلی در اصل صحتی مندرج است که موضوع و محل اجرای آن موجود باشد. درباره قراردادی که واقع شده است، می‌توان صحت و فساد را تصور کرد و گرنه نسبت به عقدی که در آینده واقع می‌شود یا در جریان وقوع است، به هیچ اصلی نمی‌توان استناد کرد تا دادرس را از جستجو و احراز شرایط تحقق آن بی‌نیاز کند.»<sup>۷۵</sup>

ایشان در ادامه با طرح این پرسش که «کدام رویداد اجتماعی است که عقد نامیده می‌شود و ارکان ظهوری که دلالت بر وقوع عقد می‌کند، چیست؟» تا بتوان آن را مشمول اصل صحت دانست، وقوع «ظاهری» و «حقوقی (و نه عرفی)» عقد را کافی می‌داند و بیان می‌کند: «بعضی از محققان، معیار تحقق عقد را «وقوع عرفی» آن پنداشته‌اند؛ بدین معنا که باید دید از دیدگاه عرف، ارکان تشکیل‌دهنده عقد چیست و کدام شرط را باید از ارکان آن شمرد. ولی باید دانست که احکام عرف گاه مبهم و گاه با نظام حقوقی متفاوت است. دادرس در پی احراز وقوع عقد در نظام حقوقی معین است تا بتواند اصلی را که آن نظام درباره عقد تمهید کرده است، به کار بندد و حکم ظاهری «صحت» را به دست آورد. ماده ۲۲۳ قانون مدنی نیز بی‌گمان به «وقوع حقوقی» عقد نظر دارد نه «وقوع عرفی» آن. منتها چون احراز تمام شرایط درستی و نفوذ عقد، حکمت تأسیس اصل را از بین می‌برد، باید آن را به «وقوع ظاهری» تعبیر کرد و همین اندازه که ارکان حقوقی عقد به ظاهر جمع آمد، آن را «واقع‌شده» دانست.

در پاسخ این سؤال که با احراز چه وقایعی عقد به ظاهر واقع می‌شود و محل اجرای صحت به وجود می‌آید؟ باید گفت رکن اساسی هر عقد، وقوع تراضی است. شرایط دیگر در اطراف این محور اصلی می‌گردد و زمینه را برای سلامت و اعتبار آن فراهم می‌آورد. پس شک در وقوع تراضی بی‌گمان شک در وقوع عقد است و استناد به اصل صحت، آن را از بین نمی‌برد: فرض کنیم اختلاف شده که آیا دو طرف هنوز در مرحله گفتگوهای مقدماتی بوده‌اند یا ایجاب و قبول را به‌طور قاطع بیان کرده‌اند. در این دعوا، نسبت به تحقق محمل و موطن اصل صحت تردید وجود دارد؛ هنوز جوهر اصلی عقد مایه نگرفته است تا بتوان وصف صحت را از عوارض آن شمرد. ناچار اصل عدم و استصحاب بقای دو عوض، نقش طبیعی خویش را بر عهده می‌گیرد و با هیچ فرض حقوقی بالاتری برخورد نمی‌کند؛ اگر تردید را اماره‌ها

و دلایل برطرف نکند، اصل عدم وقوع و فساد عقد است و مدعی وقوع و اعتبار عقد بایستی بار اثبات را به دوش کشد.»

در نهایت دکتر کاتوزیان، اصل صحت را در مقام تردید نسبت به هر امری، جز آنچه مربوط به وقوع تراضی میان طرفین است، جاری می‌داند و این‌گونه می‌آورد: «تمامی دعاوی فرعی که به‌طور مستقیم یا غیرمستقیم به تردید درباره تراضی می‌انجامد، از قلمروی اصل صحت بیرون است: مانند شک در ماهیت پیشنهاد که ایجاب است یا دعوت به مذاکره؛ تردید در اینکه پاسخ به ایجاب «قبول» است یا پیشنهاد جدید؛ تردید در اینکه آیا قبول پیش از پایان مدت اعتبار ایجاب اعلان شده است یا بعد از آن؛ تردید در این باره که آیا برنده شدن مزایده ایجاب است یا قبول؛ شک در زنده بودن گوینده ایجاب به هنگام قبول؛ سوءتفاهم درباره نوع عقد (مانند اینکه مالک ادعا کند که آن را اجاره داده‌ام و طرف قرارداد مدعی شود که آن را خریده‌ام)؛ مطابق نبودن ایجاب و قبول درباره موضوع معین (مانند اینکه خریدار بگوید آن گلدان چینی را خریدم و فروشنده بگوید این کاسه سفالین را فروختم).

برعکس در مواردی که ادعا می‌شود بیان اراده با قصد باطنی یکسان نیست، یا اشتباه در شخصیت طرف معامله یا وصف ذاتی مورد معامله رخ داده است، یا طرف قرارداد به دلیل فشارهای خارجی (اکراه) مختار نبوده است، یا دو طرف یا یکی از آنها اهلیت عهد بستن را نداشته است یا موضوع انتقال به هنگام انعقاد پیمان مالیت یا قابلیت انتقال را دارا نبوده است، یا در مشروع بودن جهت عقد تردید می‌شود، اصل صحت عقد است و طرفی که می‌خواهد فساد عقد به‌ظاهر واقع شده را اثبات کند، باید دلیل بیاورد. همچنین در مورد وجود هر شرط فاسد در عقد و تردید در سرایت آن به ارکان معامله.»

ایشان در توضیح چرایی توسعه گستره قلمروی اصل صحت به «مصالح اجتماعی مربوط به حمایت از حسن نیت اشخاص و تأمین استقرار و استواری قراردادها» و اینکه «این امر ایجاب می‌کند که به ظنون مربوط به فساد معامله بی‌اعتنایی شود و قاعده صحت بر دعاوی سایه افکند» استناد می‌کنند.

### ۳-۲-۲- عدم اجرای اصل صحت در فرض تردید نسبت به اهلیت طرفین

دکتر گرجی بر این باور است که «بدیهی است سیره که دلیل اصلی اصل صحت است جریان ندارد مگر در موردی که به وجه معتبر احراز شود که ارکان، اعم از عرفی و شرعی در متصرفین (متعاقدين) و متصرفیه (مورد عقد) تحقق یافته باشد.» ایشان در تعریف رکن عرفی و شرعی معامله این‌گونه توضیح می‌دهد: «رکن معامله، یعنی اموری که موجب تحقق اساس معامله است، بر دو قسم است: یک قسم - چیزهایی است که از نظر عرف و عقلا مقوم عنوان معامله‌اند؛ به‌طوری که اگر وجود

نداشته باشند، از نظر عرف و عقلاً عنوان معامله تحقق پیدا نمی‌کند مانند عقل و تمییز متعاقدين و مالیت مبیع در مورد عقد که اگر یکی از اینها تحقق نداشته باشد، از نظر عرف عنوان معامله تحقق پیدا نمی‌کند. قسم دیگر - چیزهایی است که از نظر شرع، مقوم عنوان معامله‌اند؛ و اگر وجود نداشته باشند، شرعاً معامله اساس پیدا نمی‌کند؛ مانند بلوغ نسبت به متصرف و مالیت شرعی نسبت به متصرف‌فیه، اگر بلوغ یا مالیت شرعی وجود نداشته باشد، مثلاً بایع، کودک ممیز باشد یا مبیع خمر و خنزیر باشد از ظر شارع عنوان بیع تحقق پیدا نخواهد کرد.»

با این توضیحات، دکتر گرجی در خصوص گستره اصل صحت معتقد است: «[اصل صحت در جایی جریان دارد که] شک در صحت از احتمال عدم تحقق امور معتبره شرعی خارج از ارکان، مانند عبودیت، ماضویت، تساوی ایجاب و قبول و مانند اینها سرچشمه گرفته باشد، اما در صورتی که ارکان احراز نشده و منشأ شک در صحت، احتمال اختلال ارکان باشد؛ مانند شک در بلوغ، عقل و امثال اینها، جریان سیره در آن مشکوک، بلکه معلوم‌العدم است، اگر کسی چیزی را که مالیتش معلوم نیست، بفروشد، سیره بر حمل فعل او بر صحت وجود ندارد. سِرّ مطلب این است که اصل صحت برای اثبات صحت فعلی تشریح شده و پیداست که صحت فعلی اقتضا دارد قابلیت و اهلیت صحت محرز باشد.»

ایشان در ادامه می‌افزاید: «میزان کلی در باب اجرا اصالة الصحة این است که در هر مورد که منشأ شک در صحت عمل غایر، شک در اهلیت تصرف باشد، اصالة الصحة جاری نخواهد بود و در جایی که منشأ شک چیز دیگری است از این جهت مانعی از جریان اصالة الصحة وجود نخواهد داشت.»<sup>۷۶</sup> با این توضیحات، دکتر گرجی قائل به این است که طرفین معامله نیز جزء ارکان معامله بوده و در صورت تردید در اهلیت ایشان، اساساً قراردادی منعقد نشده تا بخواهیم اصل صحت را نسبت بدان جاری کنیم.

دکتر لنگرودی نیز، در این خصوص که اصل صحت در شرایط تردید در احراز اهلیت طرفین جاری نیست، با دکتر گرجی هم‌رأی است. ایشان شروط مربوط به صحت عقد را در رابطه با اجرای اصل صحت به سه گروه تقسیم کرده است: ۱- شروط مربوط به عوضین که به اعتقاد ایشان درباره تردید در مالیت داشتن و قابلیت انتقال، اصل صحت جاری نمی‌شود، ولی نسبت به شک در معلوم بودن و قابل تسلیم بودن مورد معامله رعایت می‌شود. ۲- شروط مربوط به متعاقدين که در مورد تردید در «اهلیت» اصل صحت را جاری نمی‌داند و شک در سایر اوصاف مانند اختیار (اکراه) را در قلمروی اصل صحت قرار

۷۶. ابوالقاسم گرجی، اندیشه‌های حقوقی، مفاهیم بنیادین حقوق مدنی و جزایی (تهران: انتشارات مجد، ۱۳۹۲)، ۱۸۸-

می‌دهد. ۳- شروط مربوط به عقد، مانند موالات بین ایجاب و قبول و مشروع بودن جهت که به شک در وجود آنها بر مبنای اصل صحت اعتنا نمی‌شود.<sup>۷۷</sup>

استاد سیدحسن امامی درباره تردید نسبت به صحت و فساد معامله‌ای که مجنون ادواری انجام داده است، آورده‌اند که اصل، فساد معامله است و مدعی صحت باید ثابت کند که معامله در افاقه واقع شده است. ایشان در توجیه این نظر و پاسخ به ایراد کسانی که مورد را مضمول اصل صحت می‌دانند، بیان می‌کنند: «اصاله‌الصحه در موردی جاری می‌گردد که در یکی از ارکان صحت معامله اصل عقلی معارضی جاری نشود که با عمل به آن، حکم به فقدان آن بازگردد، چنانکه در مورد مذکور می‌باشد که موجب تردید در صحت معامله، شک در وجود اهلیت یکی از متعاملین است که سابقاً مجنون بوده است که با استصحاب جنون، حکم به جنون او در حین معامله می‌شود و محلی برای جریان اصاله‌الصحه باقی نمی‌ماند؛ بنابراین اصل بطلان معامله با مجنون ادواری است تا مدعی صحت ثابت نماید که عقد در زمان افاقه واقع شده است.»<sup>۷۸</sup>

حقوق‌دان دیگری در تأیید اینکه اصل صحت در شرایط تردید نسبت به احراز اهلیت طرفین جاری نمی‌شود، آورده است: «هرگاه تردید شود که طرف قرارداد قصد انشا یا رضا داشته یا جهت معامله نامشروع بوده یا معامله به قصد فرار از دین تشکیل شده، اصل صحت جاری می‌شود به شرط اینکه به هنگام تشکیل قرارداد به حسب ظاهر، شرایط موجود باشند. ولی چون اهلیت استیفای طرف به هنگام معامله باید احراز شود (مواد ۲۱۰ و ۲۱۱ قانون مدنی) به استناد اصل صحت نمی‌توان اهلیت طرف را احراز و به صحت معامله حکم کرد.»<sup>۷۹</sup>

### ۳-۳- اجرای اصل صحت در قرارداد هوشمند

حسب توضیحاتی که پیش‌تر ارائه شد، این امر را می‌توان به‌عنوان یک گزاره عام در قرارداد هوشمند مفروض دانست که طرفین قرارداد در شرایطی به انعقاد قرارداد با یکدیگر روی می‌آورند که نه‌تنها علم تفصیلی نسبت به یکدیگر ندارند؛ بلکه حتی علم اجمالی و کلی نیز برایشان حاصل نمی‌شود. تأکید بر گزاره عام از جهت اشاره به این نکته روشن بود که در صورتی که طرفین قرارداد بخواهند می‌توانند این مطالبه را از یکدیگر مطرح سازند که هویتشان افشا شود؛ لیکن نکته مهم این است که آنچه در عرصه

۷۷. محمدجعفر جعفری لنگرودی، دائرةالمعارف حقوق مدنی و تجارت، جلد ۱ (تهران: گنج دانش، ۱۳۸۸)، ۲۰۸.

۷۸. سیدحسن امامی، حقوق مدنی، جلد ۵ (تهران: انتشارات اسلامی، ۱۳۹۰)، ۳۱۰.

۷۹. سیدمرتضی قاسم‌زاده، تفسیر قانون مدنی: اسناد، آرا و اندیشه‌های حقوقی (تهران: سمت، ۱۳۹۷)، ۸۷.

عمل در مکانیسم قرارداد هوشمند رخ می‌دهد، این است که طرفین نسبت به این امر احساس استغنا کرده و بدون شناخت طرف مقابل روی به انعقاد قرارداد می‌آورند. یکی از دلایل اصلی این استغنا نیز این است که به‌طور کلی خواسته اصلی طرفین قرارداد از شناخت طرف مقابل، اطمینان یافتن از حسن اجرای قرارداد و نیز در صورت تخلف، اقامه دعوی علیه یکدیگر است. در شرایطی که قرارداد هوشمند به‌طور خودکار اجرا می‌شود و در واقع در صورت تخلف متعهد، مبلغ به‌طور خودکار به طرف مقابل عودت می‌شود، دیگر اساساً بیم عدم اجرای آن نمی‌رود تا نیاز به اتخاذ تمهیدات احساس شود. با این وصف اگر بناست در خصوص قرارداد هوشمند سخن بگوییم و حکمی در خصوص صحت و بطلان آن صادر کنیم، باید با مفروض انگاشتن توضیح مذکور، این مهم انجام شود.

از سوی دیگر می‌توان مدعی شد از منظر حقوقی، در فرض مجهول بودن اهلیت طرفین، باید حکم به بطلان معامله داد. از میان حقوق دانان، صرفاً دکتر کاتوزیان نگاهی مخالف داشتند. در تبیین ارائه‌شده توسط ایشان نیز نوعی تهافت به چشم می‌خورد؛ توضیح آنکه ایشان از یک سو معتقد است نخست «قوانین مربوط به اهلیت و حجر از قواعد مربوط به نظم عمومی است.»، دوم اینکه در فرضی می‌توان اصل صحت را جاری کرد که عقد از منظر حقوقی منعقد شده باشد و اتکا به انعقاد عرفی ناکافی است. در عین حال و از سوی دیگر، ایشان با این استناد که وقوع ظاهری عقد کافی است، احراز اهلیت طرفین را برای اینکه مدعی شویم عقدی به‌طور صحیح منعقد شده، لازم ندانسته و صرف تراضی طرفین را کافی می‌شمارند. این در حالی است که اگر بنا بر وقوع حقوقی عقد است، چه تمایزی میان قصد و اهلیت طرفین وجود دارد؟ قانون همان‌طور که وجود دو اراده انشایی را برای انعقاد قرارداد لازم تلقی کرده، حضور دو طرف دارای اهلیت را نیز ضروری می‌داند؛ بدین معنا همان‌طور که اگر در پیوند دو اراده انشایی دچار تردید شویم، اصل را بر عدم انعقاد قرار می‌گذاریم (امری که دکتر کاتوزیان نیز بر آن صحنه می‌گذارند) در صورتی که در اهلیت دو طرف معامله نیز تردید داشته باشیم، باید اصل را بر عدم گذاشته و معامله را تحقق نیافته تلقی کنیم. افزون بر این حتی اگر بنا بر احراز عرفی عقد بود، باز هم به نظر می‌رسد حداقل وجود عقل و سن برای انعقاد معامله از سوی عرف لازم دانسته می‌شود.

با این توضیحات می‌توان به جد مدعی شد که از یک سو به دلیل مجهول ماندن اهلیت طرفین معامله در قرارداد هوشمند و از سوی دیگر، عدم امکان اجرای اصل صحت در فرضی که اهلیت طرفین احراز نشده، قرارداد مذکور محکوم به بطلان است.

## نتیجه‌گیری

قرارداد هوشمند یکی از قراردادهای جدیدی است که در سالیان اخیر پا به عرصه حقوقی نهاده و بسیاری از زوایای آن باید از منظر حقوقی مورد واکاوی قرار گیرد. این قرارداد در بستر نرم‌افزارهایی منعقد می‌شود (نظیر اتریوم) که از فناوری بلاکچین بهره می‌برند؛ فلذا ناگزیر رنگ ویژگی‌های ذاتی این قرارداد را به خود می‌گیرد. از جمله این ویژگی‌ها می‌توان به انعقاد قرارداد هوشمند در بستر یک دفتر کل توزیع شده اشاره کرد که عموماً افراد در آن از طریق کدهای دیجیتال و کلیدهای عمومی و خصوصی با یکدیگر در تعامل اند و از هویت واقعی یکدیگر بی‌خبرند.

یکی از شرایط اساسی صحت هر معامله، اهلیت طرفین است؛ این در حالی است که این امر عموماً در قرارداد هوشمند برای طرفین معامله مجهول باقی می‌ماند. با این وصف این سؤال اساسی بروز می‌کند که با توجه به عدم احراز اهلیت طرفین، آیا امکان استناد به اصل صحت در قرارداد هوشمند وجود دارد یا خیر. در این راستا به بررسی آرای فقها و حقوق‌دانان پرداختیم. پیشینه فقهی اصل صحت نشان می‌دهد که فقها ضمن پذیرش آن، در خصوص گستره شمول اصل اختلاف نظر دارند و از همین رو، دشوار است با تتبع در آرای فقها، در خصوص دایره شمول قطعی آن اظهار نظر قطعی کرد. لیکن همان‌طور که مشاهده شد، عمده حقوق‌دانان بر این امر اتفاق نظر داشتند که اصل صحت در فرضی که نسبت به اهلیت طرفین تردید وجود دارد، جاری نمی‌شود. با توضیحات فوق می‌توان با جدیت مدعی شد که اصولاً قرارداد هوشمند، به دلیل مجهول ماندن هویت و عدم احراز اهلیت طرفین، باطل بوده و امکان اجرای اصل صحت در آن وجود ندارد. روشن است که این قاعده عام بوده و در شرایط خاص، نظیر موردی که طرفین به هر طریقی خارج از سازکار اصلی این قرارداد، پی به اهلیت یکدیگر ببرند، از این مانع‌رهایی جسته و قراردادشان صحیح خواهد بود.

## فهرست منابع

### الف) منابع فارسی

- امامی، سیدحسن. حقوق مدنی، جلد ۵. تهران: انتشارات اسلامیه، ۱۳۹۰.
- جعفری لنگرودی، محمدجعفر. دائره‌المعارف حقوق مدنی و تجارت، جلد ۱. تهران: گنج دانش، ۱۳۸۸.
- خوانساری رسول و وهاب قلیچ. بررسی ابعاد فقهی و حقوقی به‌کارگیری قراردادهای هوشمند در نظام مالی ایران. تهران: پژوهشکده پولی و بانکی بانک مرکزی جمهوری اسلامی ایران، ۱۳۹۹.
- شیروی، عبدالحسین و مرتضی محمدی. «تشکیل قراردادها از طریق نمایندگی سامانه هوشمند». حقوق تطبیقی، ۱۶(۱۳۸۸)، ۲۳-۴۶.  
[https://law.mofidu.ac.ir/article\\_46887.html](https://law.mofidu.ac.ir/article_46887.html)
- صفایی، سیدحسین. حقوق مدنی: قواعد عمومی قراردادها. تهران: میزان، ۱۳۹۷.
- عباسی، جواد. بلاکچین: آشنایی با مفاهیم بنیادین. تهران: مؤسسه کتاب مهربان نشر، ۱۳۹۷.
- قاسم‌زاده، سیدمرتضی. تفسیر قانون مدنی: اسناد، آرا و اندیشه‌های حقوقی. تهران: سمت، ۱۳۹۷.
- کاتوزیان، ناصر. دوره حقوق مدنی، قواعد عمومی قراردادها، جلد دوم: انعقاد و اعتبار قرارداد نظریه بطلان و عدم نفوذ. تهران: شرکت سهامی انتشار، ۱۳۹۴.
- گرچی، ابوالقاسم. اندیشه‌های حقوقی، مفاهیم بنیادین حقوق مدنی و جزایی. تهران: انتشارات مجد، ۱۳۹۲.
- مظاهری کوهانستانی، رسول. مطالعه تطبیقی امضای الکترونیکی در حقوق ایران و مقررات آن‌سیترال. تهران: انتشارات جنگل، ۱۳۹۲.
- مافی، همایون و مهدی ناصر. «واکوی مکانیسم احراز اهلیت متعاملین در پیاده‌سازی قراردادهای هوشمند در حقوق ایران». پژوهشنامه بازرگانی، ۲۵، ۹۸(۱۴۰۰)، ۲۷۹-۳۲۰.  
doi: 10.22034/ijts.2021.245373

### ب) منابع عربی

- انصاری، مرتضی. فرائد الاصول. قم: مجمع الفکر الاسلامی، ۱۴۱۹.
  - حسینی عاملی، سیدمحمدجواد. مفتاح الکرامه فی شرح قواعد العلامه. قم: دفتر انتشارات اسلامی، ۱۳۹۱.
  - خوبی، دراسات فی علم الاصول، تقریر سیدعلی هاشمی شاهرودی. قم: مؤسسه دائره‌المعارف فقه اسلامی، ۱۴۲۶.
  - طوسی، محمدبن حسن. المبسوط فی فقه الامامیه، جلد ۲. قم: دفتر انتشارات اسلامی، ۱۳۸۶.
  - حلی، حسن بن یوسف. قواعد الاحکام، قم: دفتر انتشارات اسلامی، ۱۳۷۰.
  - مشکینی، علی. المنافع العامه. تهران: انتشارات یاسر، ۱۳۴۸.
  - نائینی، محمدحسین. فوائد الاصول، جلد ۴. قم: دفتر انتشارات اسلامی، ۱۳۷۶.
  - نجفی، محمدحسن. جواهر الکلام فی شرح شرائع الإسلام، جلد ۲۳. قم: مؤسسه نشر اسلامی، ۱۴۳۲ق.
- ج) منابع انگلیسی

- Bohme, Rainer, Nicolas Christin, Benjamin Edelman and Tyler Moore. "Bitcoin: Economics, Technology, and Governance". *Journal of Economic Perspectives*, 29, 2(2015), 213-238.

- Daveis, Paul S. "Smart contracts" in Contents of Commercial Contracts: Terms Affecting Freedoms. Oxford: Hart Publishing, 2020

- Davidson, Sinclair, Primavera de Filippi & Jason Potts. "Economics of Blockchain". Public Choice Conference, May 2016, Fort Lauderdale, United States. <https://hal.science/hal-01382002/document>
- Durovic, Mateja & Andre Janssen, "The Formation of Smart Contracts and Beyond: Shaking the Fundamentals of Contract Law", In book *Smart Contracts and Blockchain Technology: Role of Contract Law*". Cambridge: Cambridge University Press, 2019. Available at: [https://www.researchgate.net/publication/327732779\\_The\\_Formation\\_of\\_Smart\\_Contracts\\_and\\_Beyond\\_Shaking\\_the\\_Fundamentals\\_of\\_Contract\\_Law](https://www.researchgate.net/publication/327732779_The_Formation_of_Smart_Contracts_and_Beyond_Shaking_the_Fundamentals_of_Contract_Law)
- Ethereum Daily Verified Contracts Chart. last modified Jan 14, 2023. Available at <https://etherscan.io/chart/verified-contracts>.
- FATF. FATF Report to G20 Finance Ministers and Central Bank Governors (Paris: Financial Action Task Group, 2018. <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/FATF-G20-FM-CBG-March-2018.pdf.coredownload.pdf>
- FATF. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paris: Financial Action Task Group, 2021.
- Kristen, Silverberg. *Getting Smart: Contracts on the Blockchain*. Washington: Institute of International Finance, 2016.
- Lauslahti, Kristian, Juri Mattila & Timo Seppala. "Smart Contracts - How will Blockchain Technology Affect Contractual Practices". *ETLA Reports*, 68(2018), 3-27. Accessed 24 Dec 2018. <http://dx.doi.org/10.2139/ssrn.3154043>
- Law Commission. *Smart legal contracts: Advice to Government*. London: Crown, 2021.
- Schrepel, Thibault. "Collusion by Blockchain and Smart Contracts". *Harvard Journal of Law and Technology*, 33, 1(2019), 66-118. <http://dx.doi.org/10.2139/ssrn.3315182>
- UK Jurisdiction Taskforce. *Legal Statement on Cryptoasset and Smart Contracts*. London: The LawTech Delivery Panel, 2019.
- Winn, K. Jane and Benjamin Writht. *The law of Electronic Commerce*. New York: Wolters Kluwer, 2002.
- Wood, Gavin. "Ethereum: A secure decentralized generalized transaction ledger", *Ethereum Project Yellow Paper*, 151(2014), 1-32.
- Wright, Aaron and Primavera De Filippi. "Decentralized Blockchain Technology and the Rise of Lex Cryptographia". SSRN, (2015), Accessed 25 Jul 2017, DOI:10.2139/ssrn.2580664
- Zheng, Gavin. *Etherium Smart Contract Development in Solidity*. Singapore: Springer, 2021.